SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
GEORGE F. BISHOP (CA Bar No. 89205)
gbishop@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
yorio@carrferrell.com
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

PRIVASYS, INC.

Plaintiff,

v.

AMERICAN EXPRESS COMPANY and AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.,

Defendants.

Case No. _____

ORIGINAL COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff PrivaSys, Inc. ("PrivaSys" or "Plaintiff") hereby files its complaint against Defendants American Express Company and American Express Travel Related Services Company, Inc., (collectively "American Express" or "Defendants") for patent infringement. For its complaint, Plaintiff alleges, on personal knowledge as to its own acts and on information and belief as to all other matters, as follows:

PARTIES

1. PrivaSys is a corporation organized under the laws of the State of Delaware, and has its principal place of business in Newbury Park, California. PrivaSys is and at all pertinent times was the assignee and owner of the patent at issue in this case.

2. Defendant American Express Company is a corporation organized under the laws of the State of New York, and has its principal place of business in New York, New York.

3. Defendant American Express Travel Related Services Company, Inc., a wholly-owned subsidiary of the American Express Company, is a corporation organized under the laws of the State of New York, and has its principal place of business in New York, New York.

JURISDICTION AND VENUE

4. This complaint asserts a cause of action for patent infringement under the Patent Act, 35 U.S.C. § 271. This Court has subject matter jurisdiction over this matter by virtue of 28 U.S.C. § 1338(a). Venue is proper in this Court by virtue of 28 U.S.C. § 1391(b) and (c) and 28 U.S.C. § 1400(b).

5. This Court has personal jurisdiction over American Express because it provides infringing products and services in the Northern District of California and American Express has a regular and established place of business in this district.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Civil LR 3-2(c), this case should be subject to district-wide assignment because it is an Intellectual Property Action.

BACKGROUND

The Pervasive Payment Card Fraud Problem

7. For the past 40 years, until relatively recently, payment cards (*e.g.*, credit, charge and debit cards) have been inanimate pieces of plastic. Each card has a primary account number in embossed characters, information about the cardholder also embossed, an encoded magnetic stripe ("magstripe") on the back of the card, and a printed and visible three or four digit security code. Devices such as fobs are used in addition to cards to conduct payment transactions. As used herein the term "card" includes such payment devices and the term "device" includes payment cards.

8. The magstripe contains data that can be read by magstripe readers, the terminals used by merchants at the point of sale ("POS"). When a merchant swipes a card, a magnetic head reads the encoded data and then transmits the data to the issuing financial institution with an authorization request. "Track 1" data on the magstripe typically contains the customer's name, account number, expiration date, and a "discretionary data" field to be used by the issuing bank. "Track 2" data contains the account number, expiration date, and another "discretionary data" field, all of which must fit within approximately 40 digits of space.

9. A person who obtains the Track 1 and Track 2 account information and the printed security code has all the information that he needs to manufacture a counterfeit card. An increasing form of fraud consists of collecting valid account numbers, either through "skimming" (*e.g.*, collecting card numbers electronically) or through data compromise (e.g.,

computer hacking) and then using the account numbers and printed security code to manufacture counterfeit cards. Payment card fraud using such techniques costs payment card networks and banks – and ultimately the cardholders – many billions of dollars a year.

10. In the last few years, major payment card networks, including American Express, Visa and MasterCard, began to offer contactless cards or devices, *i.e.*, payment cards and devices that do not need to be swiped through a magnetic reader in order to conduct a transaction. These devices commonly contain a small computer chip and a contactless means of communication such as a radio-frequency antenna (RF) that allows a reader to receive data from the device when it is placed in proximity to the reader (typically within a few centimeters), and may send standardized magnetic stripe Track 1 or Track 2 data streams, *i.e.*, data is packaged as per the existing magnetic stripe legacy system protocols. Contactless devices are, if anything, more vulnerable to fraud, as, *e.g.*, the radio signal can be intercepted and the account data stolen.

11. Payment card fraud is being addressed in Europe and in Asia, in part, through the adoption of "smart cards." A smart card is a payment card equipped with a secure chip, possessing internal data processing functionality. Smart cards are more difficult to duplicate than conventional cards, and they have intrinsic security protection. In Europe, MasterCard and Visa have advanced smart cards through a joint venture known as EMVCo. ("EMV").

12. While smart cards offer many benefits, they cannot be read by conventional magstripe POS terminal readers. Instead, smart cards require new, more sophisticated terminals. In essence, full smart card adoption requires wholesale replacement of the existing POS magstripe terminals. This "re-terminalization" is expensive but essential to widespread smart card adoption.

13. Payment card networks have accelerated smart card adoption in Europe through what is known as "liability shift." In the United States, a POS merchant is not liable for loss when a fraudulent card is used in a "card present" transaction, so long as he properly obtains a "personal identification number" ("PIN") or a signature and obtains issuer authorization. Instead, the issuing bank absorbs that loss. Conversely, in countries that mandate the issuing banks release smart cards, a POS merchant in Europe bears the fraud loss unless he has invested in a smart card terminal, even if he innocently accepts a fraudulent card. Shifting the fraud loss to the merchant gives the merchant a strong incentive to invest in new smart card terminals.

14. Payment card networks have been unable to introduce smart cards in the United States. In considerable part, this is due to the enormous cost of re-terminalization, estimated to be in the vicinity of $12-13 billion. Because payment card networks have been unable to shift the fraud loss to POS merchants, those merchants lack the economic incentive to invest in new smart card terminals and have generally declined to do so.

PrivaSys' Solution To Payment Card Fraud

15. PrivaSys was founded to develop innovative ways to reduce payment card fraud while working within the existing legacy system of magstripe readers and transaction networks, and has developed solutions that are equally effective for contactless cards and devices as they are for magstripe devices. PrivaSys understood that smart cards would be adopted slowly if at all in this country, which gave rise to a compelling need to make the legacy system itself more secure. Prior security approaches, *e.g.*, card holograms or printed security codes, were easily circumvented, as they were static and unchanging. Thus, PrivaSys invented a new approach that would allow the card itself to become the center of

innovation. Re-terminalization is unnecessary because data is received from the card in the traditional magnetic stripe data packet format.

16. The PrivaSys system creates an authentication code that is unique to each card and each transaction. The data are transmitted to the reader by a signal from the card. Because a counterfeit card lacks the ability to generate this unique code, or watermark, the issuing bank or network knows to reject the fraudulent transaction.

17. The PrivaSys method works as follows:

- Each card securely stores a card-specific, cryptographic key on a chip.
- Each card contains a "counter" that increments with every use or attempted use of the card.
- Each card contains a cryptographic algorithm, to calculate an authentication code.
- The information is processed through a triple-DES (or 3DES) encryption algorithm. The output of this algorithm is reduced to several digits unique to the specific transaction for the given card.
- These digits are referred to as a "dynamic authentication code" (or DAC). The DAC is placed in the discretionary data field of Track 1 and/or Track 2. The DAC is then communicated along with the account number, expiration date and a request for authorization to the issuing bank, all through the existing legacy infrastructure.
- The issuing bank has backend software that reproduces the DAC computation on a per-card, per-transaction basis. When the issuing bank receives an authorization request and accompanying DAC, it computes its own DAC for that card using that card's specific cryptographic key. It then compares its issuer-generated DAC to the card-generated DAC, and approves the transaction if the two match, and the other account information appears proper.

A counterfeit card does not have the ability to create the unique, transaction-specific DAC. In this way, the PrivaSys method detects the use of counterfeit cards and denies any transaction attempted, and does so within the existing magstripe legacy system.

18. PrivaSys' fraud prevention technology is not, however, limited to the legacy magstripe reader system. PrivaSys designed it to be adaptable to a variety of communications systems and transmission means—including radio frequency (RF), mobile (cellular wireless), IR (infrared) and broadcasted magnetic stripe systems.

19. PrivaSys' technology is designed to bridge the gap between traditional credit cards and fully EMV-compliant smart cards. Because it does not require full re-terminalization, PrivaSys reasonably believed that its technology would be adopted quickly, populating the United States market with intelligent cards and payment devices. This would facilitate the ultimate transition to smart cards.

The PrivaSys Patent

20. Plaintiff owns a patent, U.S. Patent No. 7,195,154 ("'154 Patent" or "Routhenstein Patent"), issued on March 27, 2007, to inventor Larry Routhenstein covering PrivaSys' methods for providing secure transactions between a money source and its customer credit or debit card holders. A true and correct copy of the '154 Patent is attached as Exhibit "A." Plaintiff is the legal and rightful owner of the Routhenstein Patent.

21. The '154 Patent contains thirty-five (35) patent claims covering a unique and novel method for generating and validating a dynamic code with each transaction transmitted over the existing payment card networks. In general, the patent discloses a method that uses an encrypted and compressed authentication code that is dynamically calculated with each transaction and transmitted via the discretionary data field through the legacy payment card processing system and which is validated at the back end by the payment network or issuing bank.

22. PrivaSys has licensed this technology to several of American Express's principal competitors in the contactless payment card and transaction processing businesses,

including MasterCard, transaction processor First Data, Inc. and others. American Express, however, has refused to take a license.

American Express's Infringing Services

23. Plaintiff's patent application was publicly known as early as March 27, 2003, when the application was published by the Patent Office. On the issuance of the patent, American Express became aware of it through ongoing licensing discussions among counsel. Despite this knowledge, American Express has proceeded on a path of selling infringing products and services as detailed below.

24. American Express operates general purpose payment card network, card issuing and merchant acquiring and processing businesses that are global in scope. It is one of the world's largest providers of charge and credit cards to consumers, small businesses and corporations. These cards and devices, which include cards issued by American Express as well as cards issued by third-party banks and other institutions that are accepted on the American Express network, are currently issued in over 40 currencies. American Express cards and devices permit consumers to charge purchases of goods and services in most countries around the world at the millions of merchants that accept cards bearing the American Express logo. American Express, as of 2006, had 78 million cards in force, including Cards issued by third parties. Worldwide spending on American Express cards totals $561 billion.

25. The payment cards and devices offered by American Express and third-party banks include contactless cards and devices, *i.e.*, payment cards that do not need to be swiped through a magnetic reader, commonly called ExpressPay. References herein to American Express cards and devices and to ExpressPay cards and devices include all contactless cards and devices issued by American Express and all contactless cards and devices issued by

third-party banks or other institutions that bear the logos American Express, ExpressPay or other logos associated with American Express. Contactless cards contain a small computer chip, and, for example, "RF" cards contain a radio-frequency antenna (RF) that allows a reader to receive data from the device when it is placed in proximity to the reader (typically within a few centimeters). American Express's contactless cards are designed to send standardized magnetic stripe Track 1 or Track 2 data streams, *i.e.*, data is packaged as per the existing magnetic stripe legacy system protocols.

26. American Express's contactless payment protocols operate in general as follows. There is a unique cryptographic key for each American Express payment card and device. The card or device generates a unique several digit cryptogram for each and every card-specific transaction; this unique cryptogram is packaged as per existing magnetic stripe data protocols and sent in Track 1 or Track 2 data fields through the existing legacy system. The data is sent to American Express and/or to a bank where pursuant to American Express specifications the data is decrypted in the backend system and the transaction validated or denied.

27. Each step in the infringement of the '154 patent is performed by American Express or by a cardmember, merchant, financial institution or other entity whose performance is directed or controlled by American Express.

28. The use of a dynamic cryptogram is essential to the success of the American Express ExpressPay product. Absent such a cryptogram, the RF transactions could be easily skimmed or breached, and fraud would proliferate.

COUNT I
(Patent Infringement)

29. American Express has infringed and is still infringing the Routhenstein Patent by, without authority, consent, right or license, and in direct infringement of the Routhenstein Patent, making, using, offering for sale and/or selling products using the methods claimed in the patent in this country. This conduct constitutes infringement under 35 U.S.C. § 271(a).

30. In addition, American Express has infringed and is still infringing the Routhenstein Patent in this country, through, *inter alia*, its promotion of ExpressPay (and similar brand names) and agreements and cooperation with banks and merchants in distributing ExpressPay cards and devices and authenticating and processing transactions initiated from those devices and its active inducement of others to make, use, and/or sell the systems, products and methods claimed in one or more claims of the Routhenstein Patent. This conduct constitutes infringement under 35 U.S.C. § 271(b).

31. In addition, American Express has infringed and is still infringing the Routhenstein Patent in this country through, *inter alia*, providing and selling goods and services designed for use in practicing one or more claims of the Routhenstein Patent, where the goods and services constitute a material part of the invention and are not staple articles of commerce, and which have no use other than infringing one or more claims of the Routhenstein Patent. American Express has committed these acts with knowledge that the goods and services it provides are specially made for use in a manner that directly infringes the Routhenstein Patent. This conduct constitutes infringement under 35 U.S.C. § 271(c).

32. American Express's infringing conduct is unlawful and willful. American Express's willful conduct makes this an exceptional case as provided in 35 U.S.C. § 285.

33. As a result of American Express's infringement, Plaintiff has been damaged, and will continue to be damaged, until American Express is enjoined from further acts of infringement.

34. American Express will continue to infringe the Routhenstein Patent unless enjoined by this Court. Plaintiff faces real, substantial and irreparable damage and injury of a continuing nature from American Express's infringement for which Plaintiff has no adequate remedy at law.

WHEREFORE, Plaintiff prays:

(a) That this Court find American Express has committed acts of patent infringement under the Patent Act, 35 U.S.C. § 271;

(b) That this Court enter judgment that:

(i) The Routhenstein Patent is valid and enforceable and;

(ii) American Express has willfully infringed the Routhenstein Patent;

(c) That this Court issue a preliminary and final injunction enjoining American Express, its officers, agents, servants, employees and attorneys, and any other person in active concert or participation with them, from continuing the acts herein complained of, and more particularly, that American Express and such other persons be permanently enjoined and restrained from further infringing the Routhenstein Patent;

(d) That this Court require American Express to file with this Court, within thirty (30) days after entry of final judgment, a written statement under oath setting forth in detail the manner in which American Express has complied with the injunction;

(e) That this Court award Plaintiff the damages to which it is entitled due to American Express's patent infringement, with both pre-judgment and post-judgment interest;

(f) That American Express's infringement of the Routhenstein Patent be adjudged willful and that the damages to Plaintiff be increased by three times the amount found or assessed pursuant to 35 U.S.C. § 284;

(g) That this be adjudged an exceptional case and that Plaintiff be awarded its attorney's fees in this action pursuant to 35 U.S.C. § 285;

(h) That this Court award Plaintiff its costs and disbursements in this civil action, including reasonable attorney's fees; and

(i) That this Court grant Plaintiff such other and further relief, in law or in equity, both general and special, to which it may be entitled.

Dated: February 22, 2008

Respectfully submitted,

/s/ George F. Bishop

SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
GEORGE F. BISHOP (CA Bar No. 89205)
gbishop@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
yorio@carrferrell.com
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

DEMAND FOR JURY TRIAL

Plaintiff, by its undersigned attorneys, demands a trial by jury on all issues so triable.

Dated: February 22, 2008

Respectfully submitted,

___/s/ George F. Bishop_____
SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
GEORGE F. BISHOP (CA Bar No. 89205)
gbishop@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
yorio@carrferrell.com
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

DISCLOSURE OF NON-PARTY INTERESTED ENTITIES OR PERSONS

Pursuant to Civil L.R. 3-16, Plaintiff, by its undersigned attorneys, certifies that as of this date, there is no such interest to report.

Dated: February 22, 2008

Respectfully submitted,

__/s/ George F. Bishop _____
SPENCER HOSIE (CA Bar No. 101777)
shosie@hosielaw.com
BRUCE WECKER (CA Bar No. 078530)
bwecker@hosielaw.com
GEORGE F. BISHOP (CA Bar No. 89205)
gbishop@hosielaw.com
HOSIE McARTHUR LLP
One Market, 22nd Floor
San Francisco, CA 94105
(415) 247-6000 Tel.
(415) 247-6001 Fax

ROBERT J. YORIO (CA Bar No. 93178)
yorio@carrferrell.com
CARR & FERRELL LLP
2200 Geng Road
Palo Alto, CA 94303
(650) 812-3400 Tel.
(650) 812-3444 Fax

Attorneys for Plaintiff
PRIVASYS, INC.

EXHIBIT A

US007195154B2

(12) **United States Patent**
Routhenstein

(10) **Patent No.: US 7,195,154 B2**
(45) **Date of Patent: *Mar. 27, 2007**

(54) **METHOD FOR GENERATING CUSTOMER SECURE CARD NUMBERS**

(75) Inventor: **Larry Routhenstein**, Orlando, FL (US)

(73) Assignee: **PrivaSys, Inc.**, Newbury Park, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 157 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/960,715**

(22) Filed: **Sep. 21, 2001**

(65) **Prior Publication Data**

US 2003/0061168 A1 Mar. 27, 2003

(51) **Int. Cl.**
G06K 5/00 (2006.01)
G06F 17/00 (2006.01)

(52) **U.S. Cl.** **235/380**; 235/375

(58) **Field of Classification Search** 235/375, 235/380, 382; 705/18, 39, 44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,665,161 A 5/1972 Oberhart
3,845,277 A 10/1974 Voss et al.
4,016,405 A 4/1977 McCune et al.
4,102,493 A 7/1978 Moreno

(Continued)

FOREIGN PATENT DOCUMENTS

AU 732877 12/1998
EP 0 661 675 A2 7/1995
EP 0 722 241 A2 7/1996

(Continued)

OTHER PUBLICATIONS

Hogan et al. U.S. Appl. No. 60/280,776, entitled "Improved System and Method for Secure Payment Application (SPA) and Universal Cardholder Authentication," filed on Apr. 2, 2001.

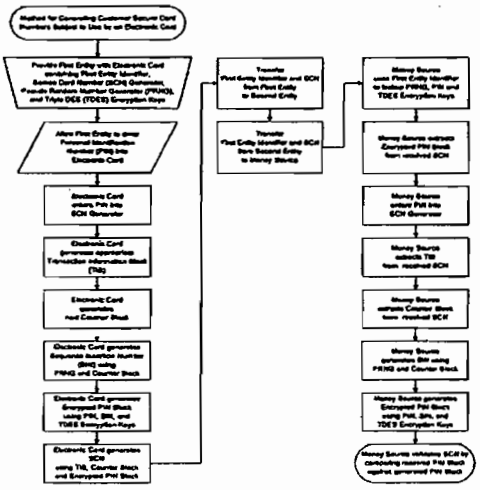
(Continued)

Primary Examiner—Thien M. Le
Assistant Examiner—April Taylor
(74) *Attorney, Agent, or Firm*—TIPS Group

(57) **ABSTRACT**

A method for providing secure transactions generates a Secure Card Number ("SCN") for a first entity that is transferred with a first entity identifier to a second entity and then to a money source that verifies that the transaction is valid by use of the first entity identifier and the SCN. The SCN includes a 0Transaction Information Block ("TIB"), a Counter Block, and an encrypted Personal Identification Number ("PIN") Block. The SCN is transferred to the money source in an account number or a non-account data field. The money source can use the TIB to determine whether the SCN should be used once or multiple times or to identify one of several physical devices, all of which are issued to the first entity, used to generate the SCN. The money source validates the SCN by duplicating the encryption process used to create an encrypted PIN Block and comparing the result to the encrypted PIN Block received with the transaction. A Triple Data Encryption Standard algorithm encrypts a PIN Block generated from a PIN, a Sequence Insertion Number ("SIN") and a known starting value. The SIN can be a combination of three seed values and a random value generated by a Pseudo Random Number Generator ("PRNG") initialized with the seed values. A Counter value is associated with the Counter Block and the seed values.

35 Claims, 1 Drawing Sheet



U.S. PATENT DOCUMENTS

4,214,230	A *	7/1980	Fak et al.	235/380
4,234,932	A	11/1980	Gorgens	
4,253,017	A	2/1981	Whitehead	
4,314,352	A	2/1982	Fought	
4,390,968	A	6/1983	Hennessy et al.	
4,437,130	A	3/1984	Hennessy et al.	
4,438,326	A	3/1984	Uchida	
4,443,027	A	4/1984	McNeely et al.	
4,458,142	A	7/1984	Bernstein	
4,614,861	A	9/1986	Pavlov et al.	
4,634,845	A	1/1987	Hale et al.	
4,650,978	A	3/1987	Hudson et al.	
4,679,236	A	7/1987	Davies	
4,689,478	A	8/1987	Hale et al.	
4,701,601	A	10/1987	Francini et al.	
4,707,594	A	11/1987	Roth	
4,742,351	A	5/1988	Suzuki	
4,755,940	A	7/1988	Brachtl et al.	
4,772,782	A	9/1988	Nonat	
4,791,283	A	12/1988	Burkhardt	
4,837,822	A	6/1989	Crosley et al.	
4,849,613	A	7/1989	Eisele	
4,868,376	A	9/1989	Lessin et al.	
4,918,631	A	4/1990	Hara et al.	
4,926,480	A	5/1990	Chaum	
4,928,001	A	5/1990	Masada	
4,959,788	A	9/1990	Nagata et al.	
4,960,982	A	10/1990	Takahira	
4,990,759	A	2/1991	Gloton et al.	
5,130,519	A	7/1992	Bush et al.	
5,168,520	A	12/1992	Weiss	
5,192,947	A	3/1993	Neustein	
5,220,501	A	6/1993	Lawlor et al.	
5,317,636	A	5/1994	Vizcaino	
5,371,797	A	12/1994	Bocinsky, Jr.	
5,373,558	A	12/1994	Chaum	
5,375,037	A	12/1994	Le Roux	
5,412,192	A	5/1995	Hoss	
5,426,283	A	6/1995	Berthozat et al.	
5,434,398	A	7/1995	Goldberg	
5,434,919	A	7/1995	Chaum	
5,438,186	A	8/1995	Nair et al.	
5,440,108	A	8/1995	Tran et al.	
5,444,616	A	8/1995	Nair et al.	
5,448,047	A	9/1995	Nair et al.	
5,455,407	A	10/1995	Rosen	
5,471,045	A	11/1995	Geronimi	
5,473,690	A	12/1995	Grimonprez et al.	
5,497,411	A	3/1996	Pellerin	
5,538,442	A	7/1996	Okada	
5,557,518	A	9/1996	Rosen	
5,568,121	A	10/1996	Lamensdorf	
5,578,808	A	11/1996	Taylor	
5,585,787	A	12/1996	Wallerstein	
5,590,038	A	12/1996	Pitroda	
5,590,197	A	12/1996	Chen et al.	
5,623,552	A	4/1997	Lane	
5,627,355	A	5/1997	Rahman et al.	
5,655,008	A	8/1997	Futch et al.	
5,671,280	A	9/1997	Rosen	
5,689,247	A	11/1997	Welner	
5,745,555	A	4/1998	Mark	
5,754,652	A	5/1998	Wilfong	
5,754,653	A	5/1998	Canfield	
5,754,656	A	5/1998	Nishioka et al.	
5,761,309	A	6/1998	Ohashi et al.	
5,790,677	A	8/1998	Fox et al.	
5,818,030	A	10/1998	Reyes	
5,825,871	A	10/1998	Mark	
5,831,862	A	11/1998	Hetrick et al.	
5,834,747	A	11/1998	Cooper	
5,834,756	A	11/1998	Gutman et al.	
5,844,497	A	12/1998	Gray	
5,850,442	A	12/1998	Muftic	
5,883,810	A	3/1999	Franklin et al.	
5,884,271	A	3/1999	Pitroda	
5,905,246	A	5/1999	Fajkowski	
5,913,203	A	6/1999	Wong et al.	
5,915,226	A	6/1999	Martineau	
5,917,168	A	6/1999	Nakamura et al.	
5,936,226	A	8/1999	Aucsmith	
5,936,541	A	8/1999	Stambler	
5,937,394	A	8/1999	Wong et al.	
5,940,511	A	8/1999	Wilfong	
5,953,710	A	9/1999	Fleming	
5,955,961	A	9/1999	Wallerstein	
5,956,699	A	9/1999	Wong et al.	
5,991,412	A	11/1999	Wissenburgh et al.	
6,000,832	A *	12/1999	Franklin et al.	700/232
6,003,763	A	12/1999	Gallagher et al.	
6,012,634	A	1/2000	Brogan et al.	
6,012,636	A	1/2000	Smith	
6,018,717	A	1/2000	Lee et al.	
6,024,288	A	2/2000	Gottlich et al.	
6,029,150	A	2/2000	Kravitz	
6,029,890	A	2/2000	Austin	
6,032,134	A	2/2000	Weissman	
6,038,492	A	3/2000	Nichols et al.	
6,047,268	A	4/2000	Bartoli et al.	
6,050,493	A	4/2000	Fertig	
6,068,184	A	5/2000	Barnett	
6,068,192	A	5/2000	McCabe et al.	
6,072,870	A	6/2000	Nguyen et al.	
6,075,861	A	6/2000	Miller, II	
6,078,888	A	6/2000	Johnson, Jr.	
6,078,902	A	6/2000	Schenkler	
6,089,451	A	7/2000	Krause	
6,098,053	A	8/2000	Slater	
6,101,477	A	8/2000	Hohle et al.	
6,111,953	A	8/2000	Walker et al.	
6,122,625	A	9/2000	Rosen	
6,132,799	A	10/2000	Comiglion et al.	
6,163,771	A	12/2000	Walker et al.	
D436,620	S	1/2001	Webb et al.	
6,188,309	B1	2/2001	Levine	
6,205,436	B1	3/2001	Rosen	
6,206,293	B1	3/2001	Gutman et al.	
RE37,122	E	4/2001	Levine et al.	
6,213,403	B1	4/2001	Bates, III	
6,215,665	B1	4/2001	Martin	
6,224,109	B1	5/2001	Yang	
6,227,447	B1	5/2001	Campisano	
6,230,977	B1	5/2001	Johnson	
6,257,486	B1	7/2001	Teicher et al.	
6,327,578	B1	12/2001	Linehan	
6,332,134	B1	12/2001	Foster	
6,339,766	B1	1/2002	Gephart	
6,343,284	B1	1/2002	Ishikawa et al.	
6,394,343	B1	5/2002	Berg et al.	
6,425,523	B1 *	7/2002	Shem-Ur et al.	235/380
6,518,927	B2	2/2003	Schremmer et al.	
6,574,730	B1	6/2003	Bissell et al.	
6,607,127	B2 *	8/2003	Wong	235/451
6,636,833	B1	10/2003	Flitcroft et al.	
6,805,288	B2 *	10/2004	Routhenstein et al.	235/380
6,834,270	B1 *	12/2004	Pagani et al.	705/65
6,915,279	B2	7/2005	Hogan et al.	
6,990,470	B2	1/2006	Hogan et al.	
7,058,611	B2	6/2006	Kranzley et al.	
2001/0034720	A1	10/2001	Armes	
2001/0047335	A1 *	11/2001	Arndt et al.	705/44
2002/0035548	A1	3/2002	Hogan et al.	
2002/0083010	A1	6/2002	Kim	
2002/0120584	A1	8/2002	Hogan et al.	

2003/0120615 A1 6/2003 Kuo

FOREIGN PATENT DOCUMENTS

EP	1 017 030	7/2000
EP	1 028 401	8/2000
JP	355143679 A	11/1980
JP	402148374 A	6/1990
JP	405040864 A	2/1993
WO	WO 92/16913	10/1992
WO	WO 99/05633	2/1999
WO	WO 99/38129	7/1999
WO	WO 99/49424	9/1999
WO	WO 99/57675	11/1999
WO	WO 00/25262	5/2000
WO	WO 00/30048	5/2000
WO	WO 00/33497	6/2000
WO	WO 00/49586	8/2000
WO	WO 00/52900	9/2000
WO	WO 00/54208	9/2000
WO	WO 01/46902 A1	6/2001
WO	WO 01/50429 A1	7/2001
WO	WO 01/54082 A1	7/2001
WO	WO 01/69556	9/2001
WO	WO 01/71675	9/2001
WO	WO 01/78024	10/2001

OTHER PUBLICATIONS

Hogan et al U.S. Appl No. 60/255168, entitled "Method and System for Conducting Secure Electronic Commerce Transactions," filed on Aug. 14, 2000.

Hogan et al U.S. Appl. No. 60/226,227, entitled "Method and System for Conducting Secure MasterCard Payments Over a Computer Network," filed on Aug. 18, 2000.

Hogan et al U.S. Appl. No. 60/213,063, entitled "An Improved Method and System for Conducting Secure Payments Over a Computer Network," filed on Jun. 21, 2000.

Hogan et al U.S. Appl. No. 09/809,367, entitled "Method and System for Secure Payments Over a Computer Network," filed on Mar. 15, 2001.

Hogan et al U.S. Appl. No. 60/195,963, entitled "Method and System for Conducting Secure Payments Over a Computer Network," filed on Apr. 11, 2000.

Hogan et al. U.S. Appl. No. 60/274,785, entitled "System and Method for Secure Payment Application (SPA) and Universal Cardholder Authentication," filed on Mar. 9, 2001.

Hogan et al. U.S. Appl. No. 60/295,630, entitled "Method and Process for a Secure Payment Application Using a Universal Cardholder Authentication Field," field on Jun. 4, 2001.

Hogan et al. U.S. Appl. No. 60/307,575, entitled "Method and System for Conducting Transactions Over a Communication Network Using a Secure Payment Application,"filed on Jul. 24, 2001.

Hogan et al. U.S. Appl., entitled "Method and System for Conducting Secure Electronic Commerce Transactions," filed on Jun. 22, 2000.

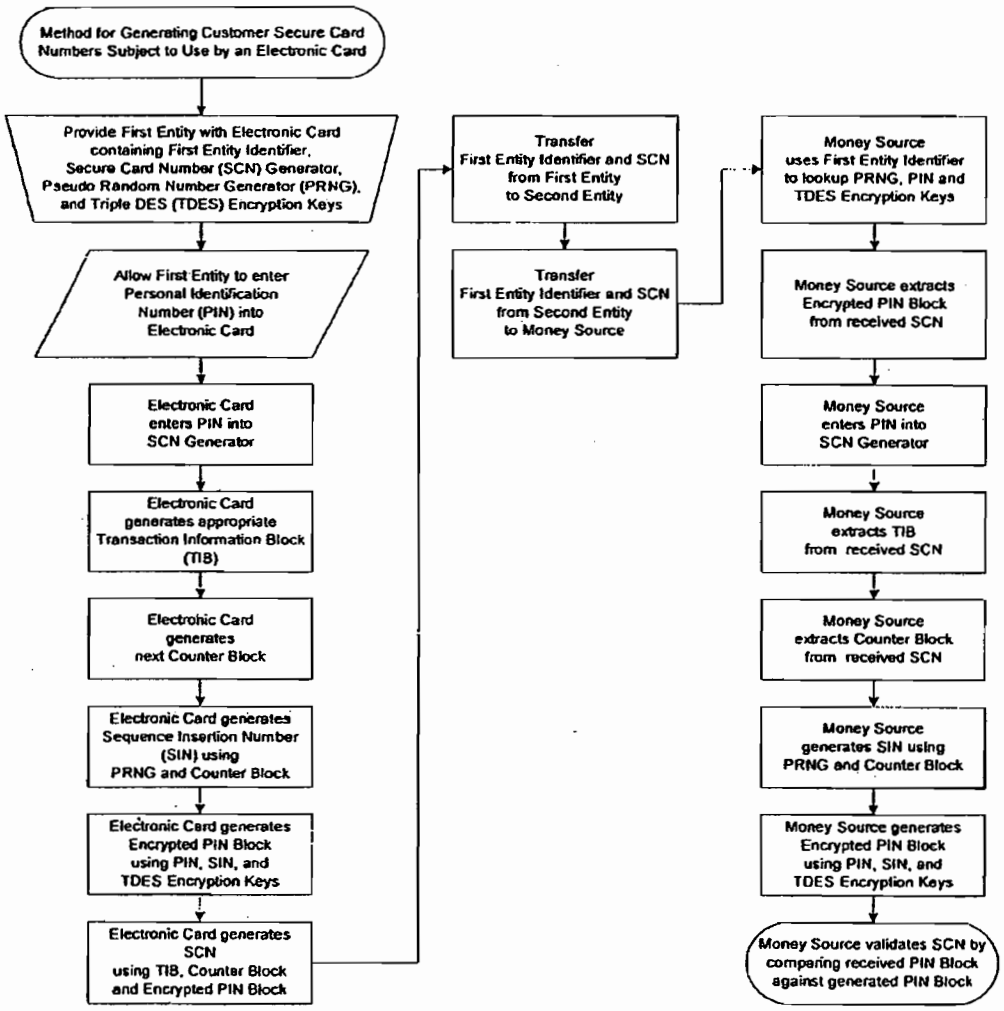
Hogan, USPTO File Wrapper March 2006 update for U.S. Appl. No. 09/833,049.

EMV '96 Integrated Circuit Card Application Specification for Payment Systems, Version 3.1.1 (May 31, 1998).

ISO/IEC JTC 1/SC 27 Information Technology - Security Techniques (May 10, 1999).

* cited by examiner

Figure 1


Method for Generating Customer Secure Card Numbers Subject to Use by an Electronic Card
Provide First Entity with Electronic Card containing First Entity Identifier, Secure Card Number (SCN) Generator, Pseudo Random Number Generator (PRNG), and Triple DES (TDES) Encryption Keys
Allow First Entity to enter Personal Identification Number (PIN) into Electronic Card
Electronic Card enters PIN into SCN Generator
Electronic Card generates appropriate Transaction Information Block (TIB)
Electronic Card generates next Counter Block
Electronic Card generates Sequence Insertion Number (SIN) using PRNG and Counter Block
Electronic Card generates Encrypted PIN Block using PIN, SIN, and TDES Encryption Keys
Electronic Card generates SCN using TIB, Counter Block and Encrypted PIN Block
Transfer First Entity Identifier and SCN from First Entity to Second Entity
Transfer First Entity Identifier and SCN from Second Entity to Money Source
Money Source uses First Entity Identifier to lookup PRNG, PIN and TDES Encryption Keys
Money Source extracts Encrypted PIN Block from received SCN
Money Source enters PIN into SCN Generator
Money Source extracts TIB from received SCN
Money Source extracts Counter Block from received SCN
Money Source generates SIN using PRNG and Counter Block
Money Source generates Encrypted PIN Block using PIN, SIN, and TDES Encryption Keys
Money Source validates SCN by comparing received PIN Block against generated PIN Block

METHOD FOR GENERATING CUSTOMER SECURE CARD NUMBERS

CROSS REFERENCE TO RELATED APPLICATIONS

The present application is related to U.S. application Ser. Nos. 09/667,081 and 09/667,089, filed Sep. 21, 2000, which are continuation-in-part applications of U.S. Ser. No. 09/659,434, filed Sep. 8, 2000, which is a continuation-in-part of U.S. Ser. No. 09/640,044, filed Aug. 15, 2000, which is a continuation-in-part of U.S. Ser. No. 09/619,859, filed Jul. 20, 2000, which is a continuation-in-part of U.S. Ser. No. 09/571,707, all of which disclosures are specifically incorporated herein by reference. This application is also related to another application being filed concurrently herewith, entitled Method for Generating Customer Secure Card Numbers Subject To Use Restrictions By An Electronic Card, Ser. No. 09/960,714.

FIELD OF THE INVENTION

The present invention is in the field of payment systems.

BACKGROUND OF THE INVENTION

Three forms of money in widespread use today throughout the world are cash, checks and payment cards (debit or credit). Each has distinct advantages, and distinct disadvantages. Cash is readily accepted, easy to use and anonymous, but it does not earn interest, it can be lost or stolen, and it is not always readily accessible. Checks are not always accepted, but they offer many advantages, since they do not have to be written until the time of payment. However, they must be physically presented and they are not anonymous. Payment cards are readily, but not always, accepted, and they offer many advantages over checks. If the card is a credit card, payment can be deferred, but the transaction is not anonymous. If the card is a debit card, payment has usually been made prior to its use, but it is anonymous. Accordingly, it is apparent that different types of money have different advantages to different persons in different situations. This may be one reason why all these forms of money are still in widespread use, and are even used by the same persons at different times.

As society and international commerce have become more dependent upon electronic transactions, money has also become more electronic. Many attempts have been made to come up with suitable forms of electronic money that mimic the physical world, or even create new forms of electronic money. However, despite the enormous need for such money, and efforts by some of the best minds and most successful companies in the world, electronic money has suffered many setbacks and been far slower to materialize than many had hoped or predicted. The reasons are many and varied, but some of the obvious reasons are security, ease of use/operation, and unwillingness of the public and/or commerce to make radical changes or embrace new technology and/or procedures. As a result, many efforts, including several potentially promising efforts, have met with failure.

Even though new forms of electronic money have been slow to develop or gain widespread acceptance, electronic payments have still moved forward. Many banks now offer some form of electronic checking. And payment cards have been used for electronic transactions in e-commerce and m-commerce (mobile commerce). Still, there is widespread concern about the safety of such transactions, and recent news stories have uncovered widespread fraudulent activity associated with use of traditional credit card numbers in e-commerce over the Internet. In addition, there is growing concern about consumer privacy, or lack thereof, due to widespread electronic profiling of consumers who make electronic payments.

Although the media has been quick to cover fraud associated with use of credit cards over the Internet, it is often overlooked, at least by the public and the media (but not the credit card companies), that the majority of fraudulent activity concerning credit cards is not associated with e-commerce activity. Most fraud occurs in the "brick and mortar" world, and the numbers are daunting. Despite many attempts to combat unauthorized or fraudulent use of credit cards, it is estimated that credit card fraud now exceeds hundreds of millions, if not several billion, dollars per year. And this does not even count the cost of inconvenience to consumers, merchants and credit card issuer/providers, or the emotional distress caused to victims of such fraud, or the cost to society in terms of law enforcement and preventative activities.

Accordingly, there is a very real, long-felt need to reduce the amount of fraudulent activity that is associated with credit cards, and this need has only grown more acute as consumers and commerce search for better ways to purchase and sell goods and services via e-commerce and m-commerce. However, any solution needs to be something that is acceptable to the public at large. It should be easy to use. It should not be complicated or expensive to implement. Preferably, it should fit within the existing infrastructure, and not be something that requires a great deal of educational effort, or a radical change in behavior or habits of consumers. In other words, it should be user friendly, readily understandable and something that does not require a completely new infrastructure, which is a reason suggested by some as to why smart cards have not been widely accepted in the United States.

In addition, it is highly desirable that any solution to such problems be capable of widespread use, in many different platforms, for many different applications.

In U.S. Pat. No. 5,956,699 issued in September of 1999, Wong and Anderson were the first to introduce the methodology of a system for secure and anonymous credit card transactions on the Internet. This patent introduced a system which used an algorithm to use one's own selected Personal Identification Number (PIN) as one's own de facto digital signature. The algorithm instructs the cardholder how to insert one's PIN into one's valid credit card number before using it for any transactions on the Internet. The resultant scrambled up credit card number, which is tailored by the algorithm to having the same number of digits as before, is rendered useless on the Internet because the PIN insertion algorithm is changed automatically after every transaction. This methodology is not only capable of drastically reducing credit card fraud on the Internet, it is also capable of safeguarding one's anonymity, and thus privacy, in credit card purchases on the Internet.

After the issuance of U.S. Pat. No. 5,956,699, Wong et al. also invented an anonymous electronic card for generating personal coupons useful in commercial and security transactions, a method for implementing anonymous credit card transactions using a fictitious account name, as well as methods for generating one-time unique numbers that can be used in credit card transactions in the brick and mortar world, e-commerce, m-commerce and in many other applications.

The present invention seeks to provide new methods for generating and processing Secure Card Numbers (SCN) that can be used in all types of transactions in which a conventional credit card account number is accepted. In addition, the present invention conforms to the existing standards for PIN encryption as promulgated by the American Bankers Association (ABA), the American National Standards Institute (ANSI), the International Standards Organization (ISO), and the Federal Information Processing Standards (FIPS) Publications of the National Institute of Standards and Technology (NIST). Because the methodology is well suited for use in hardware and software applications, it has widespread applicability to many different types of transactions.

The present invention is related to the concept of customer one-time unique purchase order numbers ("Coupons") as described in U.S. Ser. No. 09/640,044. An algorithm is executed that uses a user account number, a customer sequence number, a customer permutated user key, and a Transaction Information Block (TIB) as input variables to form an SCN that is correlated with a sequence number. Combining a user key with a user account number, a user insertion key correlated with the customer sequence number, and then encrypting the result using the Triple Data Encryption Standards (TDES), forms the customer permutated user key. A random number generator generates the user insertion key that is correlated with the sequence number. The TIB may provide several pieces of information, including the conditions under which the SCN will be valid (i.e., the SCN type), additional account indentification information, and the status of the device used for SCN generation. The sequence number can be changed after each SCN is generated and a new SCN can then be generated using a new user insertion variable correlated to the changed sequence number.

After an SCN is generated, it is transferred with a first entity identifier to a second entity (which can actually be several entities), which then transfers the information to a money source. An individual SCN is verified as being valid by the money source by duplicating the generation of the customer permutated user key for the specified first entity and the specified sequence number, and then comparing it to the customer permutated user key which is embedded in the provided SCN. Additionally, the money source verifies that the specified SCN type is valid given the specific conditions of the transaction. Once verified as valid, each SCN passes through a life cycle in accordance with conventional credit card processing practices and with its SCN type, in which it may be used for various types of transactions before being retired. If a preselected number of SCNs are received by the money source and determined to be invalid (either consecutively or within a predetermined timeframe), then an invalid user account number condition is set to prevent further attempts to verify SCNs for that first entity.

A user key can be entered into an input device, and validates the user key by comparing it to a stored user key. If the entered user key is valid, the user can generate an SCN. The sequence number changes each time a user key is entered into the input device.

SUMMARY OF THE INVENTION

The present invention is generally directed to a method for providing one or more secure transactions between a first entity and at least one additional entity in which a Secure Card Number ("SCN") is generated for the first entity, then transferred with a first entity identifier to a second entity and then transferred to a money source that verifies that the transaction is valid by use of the first entity identifier and the SCN. The SCN includes a Transaction Information Block ("TIB"), a Counter Block, and an encrypted Personal Identification Number ("PIN") Block. The SCN can be transferred to the money source in an account number while the first entity identifier is transferred to the money source in a non-account data field or the first entity identifier can be transferred to the money source as an account number while the SCN is transferred to the money source in a non-account data field.

In a first, separate aspect of the present invention, the TIB can be used for invoking one or more restrictions on use of the SCN. The money source can use the TIB to determine whether the SCN should be a single-use SCN (i.e., can only be used for a single transaction by the first entity) or a multiple-use SCN (i.e., can be used for multiple transactions between the first entity and a single merchant). The TIB can also be used by the money source to identify the physcial device used to generate the SCN.

In another, separate aspect of the present invention, the money source validates the SCN by duplicating a PIN Block encryption process used to create the encrypted PIN and by then comparing the result to the encrypted PIN Block received with the transaction.

In still another, separate aspect of the present invention, the encrypted PIN Block is formed by using a Triple Data Encryption Standard algorithm ("TDES") to encrypt a PIN Block. The PIN Block can be generated from a PIN associated with the first entity, a Sequence Insertion Number ("SIN") and a starting value known to both the first entity and to the money source. The SIN can be a combination of a first set of seed values and a random value generated by a Pseudo Random Number Generator ("PRNG") that was initialized with the first set of seed values. The first set of seed values is associated with a Counter value that is associated with Counter Block.

In yet another, separate aspect of the present invention, when the SCN is a nine digit number, the TIB is a one digit number, the Counter Block is a four digit number, and the encrypted PIN Block is a four digit number. The encrypted PIN Block can be created by dividing an 8-byte Sequence Insertion Number ("SIN") into four 2-byte integers (three seed values and the random number), adding the PIN and a pre-assigned constant 4-digit value to each of the four 2-byte integers, concatenating the results to form an 8-byte input block which the TDES encrypts into an 8-byte output block, dividing the 8-byte output block into four 2-byte integers x1, x2, x3 and x4 and then using integers x1–x4 to produce the 4-digit encrypted PIN Block with a value P, wherein $P=(Ax1+Bx2+Cx3+Dx4) \bmod 10000$, each of the values A, B, C and D being pre-assigned odd integers.

Accordingly, it is a primary object of the present invention to provide a method for generating and processing customer Secure Card Numbers for use in transactions where conventional credit card numbers are accepted.

This and further objects and advantages will be apparent to those skilled in the art in connection with the detailed description of the preferred embodiment set forth below.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 illustrates a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is related to U.S. Pat. Nos. 5,913,203, 5,937,394 and 5,956,699, the disclosures of which are all specifically incorporated herein by reference.

The preferred embodiment of the present invention is adapted for use in credit card transactions, and as such can be used in connection with a wide variety of instruments that can be used in connection with such financial transactions: electronic cards, software programs used in network applications, telephones (especially telephones used in what is now being referred to as m-commerce, or mobile commerce), or even physical imprint transactions. Moreover, it can be used whether such transactions are conducted in person, face-to-face, or whether such transactions are conducted by an indirect medium, such as a mail order transaction, a transaction conducted over a computer network (for example, the Internet), or a telephone transaction.

As is the case in most financial transactions, three parties are typically involved in completed credit card transactions according to the present invention. A party presents a credit card account number with the intent to initiate a monetary payment (or credit/return). In the context of the following description, this is the first entity or customer. Another party receives the credit card account number with the intent to receive a monetary payment (or credit/return), and this party can be a single party or two or more parties. In the context of the following description, the party or parties that are receiving the credit card account number are referred to as the second entity or merchant. Finally, there is at least one party, and usually multiple parties, that serve as intermediaries to the monetary payment (or credit/return). The second entity provides the credit card account number to this party over several transactions to effect the monetary payment (or credit/return): authorization, incremental authorization, authorization reversal, settlement, and credit/return. The intermediary group of one or more parties will be referred to in the context of the following description as a money source. Thus, the money source may be one or more banks, a credit card company or any other institution involved with issuance of credit cards or bank debit cards, such as a credit union or other institution, or a money source as described in U.S. Pat. No. 5,913,203.

In connection with the preferred embodiment, it is not necessary that the first entity use a real identity, although such an option is also acceptable. Instead, a pseudonym, such as a screen name or an alias, could be used to protect the first entity's privacy and provide additional security.

Although the first entity need not use a real identity, the first entity must establish an account with a money source. When the account is established, the first entity and the money source must agree upon a payment mechanism or protocol. In the case of a credit card or a bank card, this could be done in the same fashion as exists today, and the first entity could select a fictitious account name as is explained in greater detail in co-pending U.S. patent application Ser. No. 09/619,859. It is especially preferred that two different users not be allowed to select the same fictitious account name so that a fictitious account name also represents a unique identifier. However, the preferred embodiment could also be used in connection with a prepaid account. In such a scenario, the first entity could simply purchase a prepaid card and no real identity would ever be required.

When the first entity establishes an account with the money source, a user key must be selected. The user key can be a PIN, similar to that which is currently in widespread use in the United States in connection with automated teller machines. Both the first entity and the money source must have access to the user key, which can be selected by either entity. In order to be able to retrieve this user key, the money source must create a record associated with the first entity that includes the user key and a first entity identifier (whether this be the real name of the first entity or a fictitious account name).

Once the first entity has established an account with the money source and a user key has been selected, the first entity must be supplied with the means to generate a customer SCN. As already described, this could be hardware or software, but in either case it will include a user account number, a customer random number generator that will be used to generate user insertion keys that are correlated with a customer sequence number, and TDES encryption keys.

The TDES encryption standard is the accepted standard for protecting a PIN during data transmission of financial transactions, as described by ISO 9564-1-1991 (Banking—Personal Identification Number Management and Security—PIN Protection Principles and Techniques, Section 6.2), ISO 9564-2-1991 (Banking—Personal Identification Number Management and Security—Approved Algorithms for PIN Encipherment), ANSI X9.52-1998 (Triple Data Encryption Algorithm—Modes of Operation), and FIPS PUB 46-3 (Data Encryption Standard (DES), dated 1999), the disclosures of which are specifically incorporated herein by reference.

In order to effectively use TDES for PIN encryption, the PIN must be combined with a new set of randomly generated data for each transaction. Otherwise, the encrypted PIN would always be the same value. A customer random number generator, such as the one that is described in U.S. patent application Ser. No. 09/640,044, filed Aug. 15, 2000 and which is generally known as a Linear Congruential Generator (LCG), is used for this purpose. This random number generator is algorithmic (i.e., pseudo-random)—when starting with the same set of seeds, it always produces the same sequence of numbers. It can therefore be reproduced by the money source in order to validate a given SCN. Furthermore, since this pseudo random number generator generates its values in a reproducible sequence, each of the values in the sequence can be identified by a Counter value that indicates that number's location in the sequence. The set of random numbers generated and combined with the PIN are collectively referred to as the Sequence Insertion Number (SIN).

In the real world of credit card transactions, it is not possible to assume that transactions conducted by the first entity in a given order will always be received by the money source in that same order. Therefore, the money source method of SCN validation must be based on an embedded sequence value. The Counter value is used for this purpose in the preferred embodiment.

In general, this method can be used to generate SCNs of many different lengths. In the conventional credit card processing infrastructure, a credit card number is typically 16 digits in length. Such a number comprises three subnumbers: a 6 digit Bank Identification Number (BIN), a 9-digit account number, and a 1-digit checksum number. For the purpose of being compatible with the existing credit card processing infrastructure, the SCN could be 9 digits in length, and could take the place of the account number in the conventional 16-digit credit card number.

In the preferred embodiment, the 9-digit SCN itself comprises three subnumbers: a 1 digit TIB, a 4 digit Counter

Block (which identifies the random number being used for encryption), and a 4 digit encrypted PIN Block.

The 1 digit TIB may take on up to 10 different values, each of which may indicate multiple pieces of information. The TIB can be used to determine which of a plurality of account numbers associated with the first entity should be used for the first transaction. The account numbers can represent, for example, different credit card accounts or different payment or credit cards. A first account number might be associated with the TIB value of 0, a second account number might be associated with the values of 1 and 2, a third account number might be associated with values of 3 and 4, and so forth, wherein any odd value may be restricted to a one transaction limitation while any even value may be used to invoke permission for multiple transactions at a single merchant. In the preferred embodiment, a TIB value of 0 indicates that the SCN may only be used for one transaction; any attempts to use it for subsequent transactions will result in a transaction denial from the money source. A value of 1 indicates the same transaction restrictions as 0, but also indicates that the device generating the SCN has a low battery power condition. A value of 2 indicates that the SCN may be used for multiple transactions, but only at a single merchant; any attempts to use it for subsequent transactions at a different merchant will result in a transaction denial from the money source. A value of 3 indicates the same transaction restrictions as 1, but also indicates that the device generating the SCN has a low battery power condition. Furthermore, a set of TIB values (4, 5, 6, 7) might represent the same restriction and status information as (0, 1, 2, 3), respectively, but further indicate that the transaction is associated with a different subentity (e.g., the first entity identifier identifies a married couple, and the TIB identifies each individual spouse.) Other values might also be used to enforce additional transaction restrictions in ways readily apparent to those skilled in the art.

The TIB can also be used by the money source to uniquely identify a physcial device (such as an electronic card) used to generate the SCN. This aspect of the TIB is especially useful when the money source issues more than one card to a first entity. Multiple cards might be issued to the same person (i.e., the first entity) for different uses, or multiple cards might be issued to the same person for use by different individuals (such as family members). In such instances, the TIB can identify which physical card, issued to the first entity, is used for a given transaction. When the TIB is used in this way, the TIB can be used as a customization variable to recognize multiple cards otherwise issued to a single first entity (which might also be a legal entity, such as a corporation).

The 4-digit Counter Block is unencrypted information provided so that the money source may decrypt and validate the SCN. It may be simply the actual Counter value (incremented after each use), but in the preferred embodiment, it is created by adding the Counter value to a starting value known to both the first entity and to the money source.

The 4-digit PIN Block is the encrypted information that is used to validate the fact that the SCN originated from the first entity. The PIN Block is formed using the PIN, the SIN, and a starting value known to both the first entity and to the money source. It is encrypted using TDES, which requires use of three 64-bit keys known to both the first entity and to the money source. In order to encrypt such a small number (16 bits) with such a high level of encryption (158 bits), the PIN must first be expanded to a 64 bit number, then encrypted, and finally reduced back to a 16 bit number—and in such a way that it is guaranteed to be different for each transaction.

The SIN is the product of an LCG random number generator that is initialized with three 2-byte integer seeds—the result of operating the LCG on these seeds is a 2-byte random value. The 8-byte SIN consists of the three seeds plus the random value. As a by-product of its operation, the LCG also produces three new seeds, which will be used for the next iteration of the LCG algorithm. The SIN may therefore be associated with a Counter value that indicates a unique location in the sequence of seeds and value generated by the LCG. This SIN is used as the random basis for each successively TDES-encrypted PIN Block, and guarantees a properly encrypted PIN Block for each transaction. To allow proper validation of the SCN, the Counter value stored in the Counter block is the one associated with the SIN used as the random basis for the PIN Block.

The creation of the PIN Block starts by dividing the 8-byte SIN into four 2-byte integers. The PIN and a predefined constant value are both added to each individual 2-byte integer. The results are then concatenated back again to form an 8-byte input block to the TDES algorithm, which encrypts them into an 8-byte output block. The output block is then divided back into four 2-byte integers (x1, x2, x3, x4). These four values are then used in the following formula to produce the 4-digit PIN Block value P:

Formula 1: *PRNG* Value Calculation

$$P = (Ax_1^+ Bx_2^+ Cx_3^+ Dx_4) \bmod 10000$$

In this formula, the four values (A,B,C,D) are each odd integers. The "mod" calculation is a standard modulo arithmetic operation, and works as follows: if the resulting number is greater than 10,000 (or 20,000 or 30,000, etc.), then the value of 10,000 (or 20,000 or 30,000, etc.) is subtracted from it, leaving a positive four digit value.

Once created, the SCN is transmitted along with the first entity identifier from the first entity to the second entity and, subsequently, to the money source. In one embodiment, the SCN is used in an account number that replaces the conventional credit card number, and the first entity identifier is a static 9 digit number pre-assigned to the first entity that is transferred to the money source in a non-account data field. In the case of an electronic swipe credit card transaction, the first entity identifier is dynamically encoded onto Track 1 and/or Track 2 of the magnetic stripe in the area known as the Discretionary Data Field, which comprises up to 13 digits of information. In the case of a transaction where the first entity is not present, such as a mail order, telephone order, or Internet order, the first entity identifier is transmitted as part of the Billing Address field in one of may possible forms. For example, it may be entered as "P.O. Box <first-entity-identifier".

In an especially preferred embodiment, the SCN is not used in an account number to replace the conventional credit card number, but is instead used in conjunction with it—the conventional credit card number itself functions as the first entity identifier, and the SCN is used as a dynamic digital signature to positively identify the first entity and is transferred to the money source in a non-account field of data. In this case, the SCN is transmitted either in the Discretionary Data Field of Track 1 and/or Track 2 or via the Billing Address in a card-not-present transaction.

The Money Source validates the SCN by using the first entity identifier to lookup the information necessary to reproduce the PIN Block encryption for the first entity: the TDES keys, the LCG Seeds, and the PIN. The Money source determines the Counter value by examining the Counter Block, reproduces the calculation of the PIN Block, and then compares the results to the received PIN Block to perform the actual validation.

The Money Source also validates the usage of the SCN based on the embedded TIB. It therefore enforces the various policies based on the first entity's previous transaction history: single-use, multiple-use for single merchant, card-present only.

In the embodiment when the SCN is used in an account number in place of the conventional credit card number, it passes through the standard credit card transaction lifecycle: initial authorization, potential incremental authorization, potential authorization reversal, settlement, and potential credit/return. However, in an especially preferred embodiment, the SCN is only used for initial authorization—beyond that, the Money Source performs its standard transaction processing.

The Money Source may detect fraudulent transaction attempts in various ways. In both the embodiment where the SCN replaces the conventional credit card number, the Money Source may check for re-use of single-use SCNs, use of SCNs without first entity identifiers when the card is not present, re-use of multiple-use/single-merchant SCNs at a different merchant, or SCNs with invalid PIN Blocks. Each of these cases represents a different type of fraud. The Money Source may take various actions in response to each of these types of attacks, such as disabling the account after an excessive number of fraudulent transaction attempts, or returning the code indicating that the merchant should retain the credit card being used for the transaction.

In the preferred embodiment, the Money Source detects fraudulent authorization attempts such as re-use of single-use SCNs, re-use of multiple-use/single-merchant SCNs at a different merchant, SCNs with invalid PIN Blocks, or use of the conventional credit card number on an SCN-enabled account without inclusion of an SCN when the card is not-present. This last case covers simple Internet fraud attempts, but allows, for example, a manual-entry transaction at a POS machine or an imprint transaction. After detecting fraud attempts, the Money Source may take the same types of actions as described above.

It should be noted that the preferred embodiment allows the SCN, when paired with a conventional credit card number, to be validated by back-end software that is integrated with the issuing money source's authorization and settlement processing. An issuing money source can identify an SCN-enabled credit card account in an issuer-determined fashion (e.g., a unique Bank Identification Number). It then forwards select transaction information to the SCN-enabling software, which is installed behind the issuing money source's firewall, which validates the SCN. This means that software generating the SCN can be allowed operate in isolation—it does not have to be in communication with the back-end software—and thus it can be embedded in a credit card or other standalone device.

The inventions described above can be implemented by a money source for use with an electronic card. It is preferable that every user account utilizes the same Pseudo Random Number Generator (PRNG), such as the PRNG described in P. L'Ecuyer, "Efficient and Portable Combined Random Number Generators", *Communications of the ACM*, 31(6): 742-749,774, 1988, the disclosure of which is specifically incorporated herein by reference. However, each cardholder account has a different initial seed, and thus uses a different part of the PRNG sequence. Since the PRNG has an overall period of 10^{12}, there is ample room for each account to have its own non-repeating subsequence of 10,000 values.

The PRNG is divided into two parts: seed generation (Formula 2) and value calculation (Formula 3). In these formulas (expressed using C code fragments), the set (S_x^0, S_x^1, S_x^2) is a triplet of five-digit values in the range ([1, 32362], [1,31726], [1,31656])), and represents the seed in the x^{th} location in the sequence. Z is interim storage for the pseudo random number, and PRNG[x] indicates the pseudo random number in the x^{th} location in the sequence. Note that for the practical usage of this algorithm, "x" corresponds to the current Counter value. For each transaction, Formula 2 generates the seed (based on the previous seed) and Formula 3 generates the PRNG value.

Formula 2: *PRNG* Value Calculation

$Z = S_x^0 - S_x^1;$

if $(Z > 706) Z = Z - 32362;$

$Z = Z + S_x^2;$

if $(Z < 1) Z = Z + 32362;$

$PRNG[x] = Z$

Formula 3: *PRNG* Seed Genaration

$$S_{x_1}^0 = (S_{x-1}^0 * 157) \; mod \; 32363$$

$$S_{x_2}^0 = (S_{x-1}^1 * 146) \; mod \; 31727$$

$$S_x^2 = (S_{x-1}^2 * 142) \; mod \; 31657$$

In all cases, the initial PRNG seed (which generates value 0 in the PRNG sequence) is pre-assigned to the card. Additionally, the most recently used seed is stored in Random Access Memory (RAM). Thus, when an SCN must be generated, the card runs through both Formulas 2 and 3 exactly once, and then updates the seed storage in RAM. The Counter value is also stored in RAM, and is initialized to the value of 1 at the time the card is manufactured. Multiple values of the Counter are stored to detect accidental corruption. Each time an SCN is generated, the current value of the Counter is used. The Counter is then incremented by 1, and stored again for the next use.

Since the SCN is calculated in an algorithmic fashion, it is possible to precalculate the values for a given first entity, and store them on an electronic card. This embodiment is most useful where it is more advantageous to store a large amount of data on the electronic card than it is to perform the algorithms discussed above.

Use of the SCN technology described herein is secure when it requires the cardholder to enter a PIN in order to generate a unique SCN that is valid for only one transaction, and for only the specified cardholder. At no time during the transaction is the PIN at risk. By utilizing both encryption and random number generation technologies described herein, it is possible to achieve at least a 99.9% level of protection against fraud.

Although the foregoing detailed description is illustrative of preferred embodiments of the present invention, it is to be understood that additional embodiments thereof will be obvious to those skilled in the art. For example, the same inventive concepts disclosed herein could be used in a

system in which a customer has two or more account numbers and/or identities, with the same or different user keys. In the case of an electronic card or telephone, this would allow the customer to select which account should be used (for example, to choose a business credit card for use with a business expense, a personal credit card for use with a personal expense, or a bank card at a local store for groceries and cash back). Alternatively, a customer might be permitted to use multiple user keys for the same account number and the same identity. This could allow some of the same functionality, or it could be used to classify the type or nature of the expense or transaction. Furthermore, the same SCN concept can be easily extended to non-financial transactions where user authentication is required, such as with electronic Identification cards. Further modifications are also possible in alternative embodiments without departing from the inventive concept.

Accordingly, it will be readily apparent to those skilled in the art that still further changes and modifications in the actual concepts described herein can readily be made without departing from the spirit and scope of the disclosed inventions as defined by the following claims.

What is claimed is:

1. A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) generating a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN.

2. A method as recited in claim 1, wherein the SCN is transferred to the money source in an account number and the first entity identifier is transferred to the money source in a non-account data field.

3. A method as recited in claim 1, wherein the first entity identifier is transferred to the money source as an account number and the SCN is transferred to the money source in a non-account data field.

4. A method as recited in claim 3, wherein the TIB is used for invoking one or more restrictions on use of the SCN.

5. A method as recited in claim 4, wherein the TIB is used by the money source to determine whether the SCN is a single-use SCN or a multiple-use SCN.

6. A method as recited in claim 5, wherein the TIB is used by the money source to identify a physical device used to generate the SCN.

7. A method as recited in claim 6, wherein the encrypted PIN Block is formed by using a Triple Data Encryption Standard algorithm ("TDES") to encrypt a PIN Block.

8. A device as recited in claim 7, wherein the PIN Block is generated from a PIN associated with the first entity, a Sequence Insertion Number ("SIN") and a starting value known to both the first entity and to the money source.

9. A method as recited in claim 8, wherein the SIN is a combination of a first set of seed values and a random value generated by a Pseudo Random Number Generator ("PRNG") that was initialized with the first set of seed values.

10. A method as recited in claim 9, wherein the first set of seed values consists of three seed values.

11. A method as recited in claim 10, wherein the first set of seed values is associated with a Counter value.

12. A method as recited in claim 11, wherein the Counter Block is associated with the Counter value.

13. A method as recited in claim 12, wherein the money source validates the SCN by duplicating a PIN Block encryption process used to create the encrypted PIN and by then comparing the result to the encrypted PIN Block received with the first transaction.

14. A method as recited in claim 13, wherein the SCN is a nine digit number, the SCN Type is a one digit number, the Counter Block is a four digit number, and the encrypted PIN Block is a four digit number.

15. A method as recited in claim 14, wherein the encrypted PIN Block is created by dividing an 8-byte Sequence Insertion Number ("SIN") into four 2-byte integers, adding the PIN and a pre-assigned constant 4-digit value to each of the four 2-byte integers, concatenating the results to form an 8-byte input block which the TDES encrypts into an 8-byte output block, dividing the 8-byte output block into four 2-byte integers x1, x2, x3 and x4 and then using integers x1–x4 in Formula 1 to produce the 4-digit encrypted PIN Block with a value P, wherein Formula 1 is P=(Ax1+Bx2+Cx3+Dx4) mod 10000, each of the values A, B, C and D being pre-assigned odd integers.

16. A method as recited in claim 15, wherein each of the three seed values and the random value is a 2-byte integer.

17. A method as recited in claim 16, wherein an electronic card generates the SCN.

18. A method as recited in claim 16, wherein a PIN is entered into an input device to generate the SCN.

19. A method as recited in claim 18, wherein the SCN and first entity identifier are transferred to the second entity in a form.

20. A method as recited in claim 19, wherein the SCN is transmitted through an Address Verification System Billing Address.

21. A method as recited in claim 20, wherein a unique SCN is assigned to each first entity which is valid only for mail order, telephone order, or internet transactions, and which is used for multiple transactions with multiple merchants.

22. A method as recited in claim 21, wherein the second entity uses the SCN to authenticate the first entity.

23. A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB is used for invoking one or more restrictions on use of the SCN; and

wherein the SCN is transferred to the money source in an account number and the first entity identifier is transferred to the money source in a non-account data field.

24. A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB is used for invoking one or more restrictions on use of the SCN; and

wherein the SCN is readable by a magnetic card reader.

25. A method as recited in claim 24, wherein the SCN is readable from either a Track 1 or a Track 2 of the electronic card.

26. A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB is used for invoking one or more restrictions on use of the SCN; and

wherein the TIB is used by the money source to determine which of a plurality of account numbers associated with the first entity should be used for the first transaction.

27. A method for providing a secure transaction between a first entity and a second entity comprising:

(1) generating a Secure Card Number ("SCN") for the first entity, wherein the SCN comprises a dynamic digital signature;

(2) transferring the SCN in a non-account data field and a first entity identifier in an account data field to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN.

28. A method as recited in claim 27, wherein the first entity identifier is transferred to the money source as an account number.

29. A method as recited in claim 27, wherein the dynamic digital signature is formed by using a Triple Data Encryption Standard algorithm ("TDES").

30. A method as recited in claim 27, wherein the dynamic digital signature comprises an encrypted PIN.

31. A method as recited in claim 27, wherein the dynamic digital signature is, at least in part, encrypted, and wherein the money source validates the SCN by duplicating a dynamic digital signature encryption process and by then comparing the result to the dynamic digital signature received with the first transaction.

32. A method as recited in claim 27, wherein an electronic card generates the SCN.

33. A method as recited in claim 27, wherein a PIN is entered into an input device as a part of the generation of the SCN.

34. A method as recited in claim 27, wherein a unique SCN is assigned to each first entity which is valid only for mail order, telephone order, or internet transactions, and which is used for multiple transactions with multiple merchants.

35. A method as recited in claim 27, wherein the second entity uses the SCN to authenticate the first entity.

* * * * *